65526-CN
OA

[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G06F 7/00

[12]发明专利申请公开说明书

[21]申请号 00105464.3

[43]公开日 2000年8月30日

[11]公开号 CN 1264865A

[22]申请日 2000.3.30 [21]申请号 00105464.3

[71]申请人 后健慈
地址 台湾省台北市
[72]发明人 后健慈

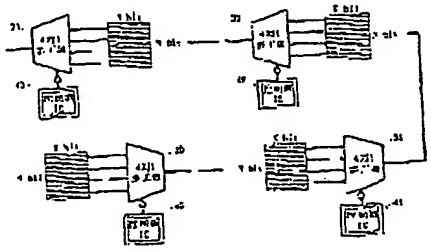
[74]专利代理机构 北京金之桥专利事务所
代理人 林建军

权利要求书1页 说明书4页 附图页数6页

[54]发明名称 未知行为模式的资料交换器运作方法及其架构

[57]摘要

本发明涉及一种未知行为模式的资料交换器动作方法及其架构，它主要是将一长串位的资料以4位划分为一组资料，交换器或缓冲器将此4位配置在划分有四个构成方块形式储存空间捣乱，每一位的位置排列组合因而产生多种变化，并对每一种变化进行编码，映像组合的编码值经一多任务器加以选择，对数据进行多层次的捣乱，藉由将原始资料的排列顺序错乱，及多任务器的多种变化，使加密安全系统的加密行为不固定，而增加非法入侵者破解的难度，以防止入侵系统。



ISSN1008-4274

权利要求书

1、一种未知行为模式的资料交换器运作方法，其特征在于它是将一长串位的资料配置在划分构成相对应位数的方块形式储存空间，并对每一方块作映像组合编码，依据 4 位的次方值（0、1、2...）的位数进行多层次的捣乱，使每一位的位置产生多种变化，并从中选择一种将原始资料的排列组合顺序错乱，使加密安全系统的加密行为不固定。

2、如权利要求 1 所述的未知行为模式的资料交换器运作方法，其特征在于该捣乱步骤可透过软件控制向左或向右旋转、或作规则性的变动。

3、如权利要求 1 所述的未知行为模式的资料交换器运作方法，其特征在于该变化的选择系于一层选择一种组合，下一层将选择距离现在的组合最远的一个组合。

4、如权利要求 1 所述的未知行为模式的资料交换器运作方法，其特征在于该捣乱的层次与变化视资料的位数而定。

5、如权利要求 1 所述的未知行为模式的资料交换器运作方法，其特征在于该方法包括下列步骤：

步骤 a、将长串位配置在划分以方块形式的相对应储存空间；

步骤 b、对 4^n 位数（n=0,1,2...）进行映像组合编码值；

步骤 c、利用一多任务器（30、31、32、33）依据编码值选择，捣乱资料的排列顺序；

步骤 d、重复步骤 b—c n 的最大次数。

6、一种未知行为模式的资料交换器架构，其特征在于它包括有：

一组依据权利要求 1 所述的未知行为模式的资料交换器运作方法所构成已编码的多层资料；

至少一个多任务器，其藉由对应的控制器集成电路控制，系对选择适当的层次数据变化进行捣乱；

一随机数产生器，其对捣乱后的资料进行随机加密。

7、如权利要求 6 所述的未知行为模式的资料交换器架构，其特征在于所述的多任务器为 4 对 1 多任务器。

说 明 书

未知行为模式的资料交换器运作方法及其架构

本发明涉及一种未知行为模式的资料交换器运作方法及其架构，特别是一种将原始资料的排列顺序进行多层次的捣乱，使加密安全系统的加密行为不固定的资料交换器的设计。

目前，建立安全、可信赖的网络环境，确保信息在网络传输过程中不易遭“黑客”非法入侵伪造、篡改或窃取是现今各网络服务提供者及电子商务的重要课题。为达到安全信息的目的，安全系统是目前业者的一道防线。

现有计算机系统的安全系统作业如图 1 所示。当资料通过资料交换器（10）（data exchanger）（或缓冲器）传输写入集成电路 20 时，随机数产生器 11（random number generator）产生随机数字，作为资料交换器加密资料的钥匙 Key。资料交换器 10 使用随机数字（加密钥匙 KEY）加密信息。加密的过程除随机数字（加密钥匙 KEY）有差异之外，每一资料的加密作业方式是完全相同的，即具有相同的行为模式。

这些资料的加密方式看起来是安全的，虽然随机数字（加密钥匙）破解（break）不易，尤其是 256 位、512 位、1024 位的随机数字（加密钥匙），确实大幅度增加了破解随机数字（加密钥匙）所需的时间。但是却忽略了另一重要的漏洞而造成致命的后果，也就是前述所有加密作业均是以随机数字加密的行为模式是一成不变的。非法入侵者事实上能藉由观察输入每一个各种可能存在的随机数字的集成电路电压变化，来推演出资料交换器 10 的行为模式（如图 2 所示）。实际上透过这种方式已有很多加密程序，如椭圆曲线密码算法 ECC(Ellipse Curve Code)、RSA(Rivest、Shamir 及 Adleman)、Block Cipher 已成功地被破解。显然，行为模式固定的加密作为方法，其安全性十分令人担忧。

本发明的主要目的，是提供一种未知行为模式的资料交换器运作方法及其架构，主要是将一长串位的资料以 4 位划分为一组资料，交换器或缓冲器将此 4 位配置在划分有四个构成方块形式的储存空间捣乱（scrambling），每一位的位置排列组合因而产生有多种变化，并对每一种变化进行编码，映像（map）组合的编码值经一多任务器（4-to-1 mux）加以选择，对数据进行多层次的捣乱，藉由将原始资料的排列顺序错乱，及多任务器的多种变化选择，使加密安全系统的加密行为不固定，以增加非法入侵者破解的困难程度，防止入侵系统。

依据前述，本发明的资料交换器的资料经过捣乱重组后，若使用一个多任务器时，经由多任务器选择，每一个位资料将具有四种变化。若使用四个多任务器时，每一个位资料将具有 4^4 种变化，多任务器的数量可视所需的保密等级加以设计。由于资料的排列顺序已被彻底且均匀地捣乱，而且是前各种变化中的一种，即使非法入侵者以前述电压变化来观察，也无法确定资料地址的顺序，其推演出的资料势必成为一个无用的资料，因此能解决现有安全系统的漏洞。

为达到上述目的，本发明提供了一种未知行为模式的资料交换器运作方法，它是将

一长串位的资料配置在划分构成相对应位数的方块形式储存空间，并对每一方块作映像组合编码，依据 4 位的次方值（0、1、2...）的位数进行多层次的捣乱，使每一位的位置产生多种变化，并从中选择一种将原始资料的排列组合顺序错乱，使加密安全系统的加密行为不固定。

本发明还提供了一种未知行为模式的资料交换器架构，其特征在于它包括有：一组依据所述的未知行为模式的资料交换器运作方法所构成已编码的多层资料；至少一个多任务器，其藉由对应的控制器集成电路控制，系对选择适当的层次数据变化进行捣乱；一随机数产生器，其对捣乱后的资料进行随机加密。

现结合附图所示的实施例详细说明本发明的结构及功能。其中：

图 1 是现有计算机系统的安全系统作业方块示意图；

图 2 是观察随机数字的集成电路电压变化的破解方式示意图；

图 3—1 至 3—3 是 Fractal 概念的方块示意图；

图 4—1 至 4—4 是本发明依据 Fractal 概念的资料格式示意图；

图 5 是本发明 256 位资料经捣乱后的资料格式示意图；

图 6 是本发明的第一实施例，其显示使用单一多任务器的资料交换器架构图；

图 7 是本发明的第二实施例，其显示使用四组多任务器的资料交换器架构图。

符号说明：

10	资料交换器	11	随机数产生器
20	集成电路	30—33	4 对 1 多任务器
40—43	控制器集成电路		

本发明的基本理论源自 Fractal 概念。如图 3—1 所示，基本的架构是由四个小的三角形所组成，任何较大的区块（如图 3—2、3—3）是包含有下列数个特征：

1. 是由基本的架构块组成；
2. 较大的区块永远看起来像基本架构块；
3. 从任何透视图法，所有的区块状似相同。

本发明将上述的特征应用于用以控制及处理不可预测及预测行为模式的资料交换器 10 或缓冲器的集成电路设计中。

首先探讨一个 4 位交换器或缓冲器 10（如图 4—1 所示）。每一个位在捣乱之后以一正方型的形式排列，如此每一个位（bit 0-3）将会有 4 种组合变化，被安排在正方形的四个角落（图中所示的 0、1、2、3 系指第几个位数）。

在本实施例中，使用了一个 4 对 1 的多任务器 30（4-to-1 mux）（如图 6 所示）去控制每一种组合，为详细说明，吾人可暂时使用：

“00” 代表  ；“01” 代表  ；“10” 代表 ；“11” 代表 ；

也就是说，当 4 对 1 多任务器 30 选择 “00” 时，这个 4 位资料交换器将会被多任务器捣乱成  。而当 “00”、“01”、“10”、“11” 在捣乱后映像（map）的这些组合将

被重新定义，且只有开发人员才会知道。

将此 4 位架构再向上扩充，如图 4—2 所示，以此 4 位所构成的正方形架构为基础，由四个 4 位的正方形构成一个 16 位区块，并将原先每一个组成 4 位的四方形视为 1 个位，因此可将其捣乱而以  表示之（如图 4—2 所示的深灰色字），于是即形成一捣乱后的 16 位资料。

再以此 16 位区块为基础，由四个 16 位的正方形构成一个 64 位的区块，并将原先每一个组成 16 位的四方形视为 1 个位，因此可将其捣乱而以  表示之（如图 4—3 所示的浅灰色字），于是即形成一捣乱后的 64 位资料。

同理，以此 64 位区块为基础，由四个 64 位的正方形构成一 256 位的区块，并将原先每一个组成 64 位的四方形视为 1 个位，因此可将其捣乱而以  表示之（如图 4—4 所示之空心字），于是即形成一捣乱后的 256 位资料。

由此可以得知，图 4—1 至 4—4 图均是由图 4—1 的 4 位架构块构成（即具有与 Fractal 概念相同的特征），吾人可以定义出层次的资料缓冲器，16 位为 4^2，64 位为 4^3，256 位为 4^4，这些数字 2、3、4 即代表资料缓冲器的层数，举例来说，一个 4 位资料缓冲器，对每一个位而言只有单层组合；64 位资料缓冲器（4^3）即包含有 3 层架构。

如前所述，每一层均能划分为 4 个均等份，因此每一个均等份可用组合数“00”、“01”、“10”、“11”来指定每一层资料，能以一个 4 对 1 多任务器 30 作指定层数及区块的控制，以此 4 种可能的变化组合，将原始资料捣乱或重组。这些变化组合可预先由开发人员任意选择预设每一层的关联性，其可依据下述原则定义出每一层的组合：

“如果一层选择一个组合，则下一层所选择将是距离现在组合最远的组合”

依据此原则，就算是 256 位缓冲器也将被限制在 4 个变化，且能被 4 对 1 多任务器 30 所控制。

下表所显示的关联表，是提供逻辑控制一 256 位缓冲器，且由此提供 4 层的组合去代表每一个位：

变化	最上层	中上层	中下层	最下层
1	00	10	11	01
2	01	11	00	10
3	10	00	01	11
4	11	01	10	00

以一笔 256bits 的资料为例，依据前述的方式以 4 位为基础构成的方块，吾人假设其编码为  （如黑色字）；构成 16 位方块的 4 个 4 位方块，吾人假设其编码为  （如深灰色字）；构成 64 位方块的 4 个 16 位方块，吾人假设其编码为  （如浅灰色字）；构成 256 位方块的 4 个 64 位方块，吾人假设其编码为  （如空心字）；资料经过重组合如图 5 所示，如此资料的排列顺序即被捣乱，除非是程序开发人员，否则将无法知道捣乱的规则，非法入侵人士所抓取的捣乱资料也成为一无用的资料。

如图 6 所示，本发明的资料交换器的架构图，N 位×N 位的资料于此以 256 位（16×16 位）为例，就前述理论，256 位资料可划分为 4 层结构（4 位、16 位、64 位及 256 位等 4 层），利用一个 4 对 1 多任务器 30 去选择变化，4 对 1 多任务器 30 的激活（enable）

则是由一控制器集成电路（controller IC）40 控制（此可由软件加以控制），控制器集成电路 40 依据变化一，随意任选其中一变化对资料进行捣乱，例如选择到最下层的“01”，系统便将 4 字节成的区块（如黑色字）内的资料进行捣乱，使原始资料的每一个位的位置顺序打乱。或者是控制器集成电路 40 依据变化一，选择到中下层“11”，系统便将 16 字节成的区块为一单位（如深灰色字）进行捣乱。以此类推，在本实施例中，此位的资料便具有四种变化的捣乱模式。

如图 7 所示，在本实施例中，使用了 4 组 4 对 1 多任务器 30—33，并以 4 位（即上表中每一种变化的最下层）为一捣乱的基本单位，并在每一个 4 对 1 多任务器 30、31、32、33 时，控制器 40、41、42、43 可以任意选择变化。举例来说，在第一个 4 对 1 多任务器 30 时，控制器集成电路 40 选择到变化一，最下层选择到“01”，系统便将 4 字节成的区块（如黑色字）内的资料进行捣乱，使原始资料的每一个位的位置顺序打乱。此捣乱后的资料再经第二个 4 对 1 多任务器 31 时，控制器集成电路 41 可以任意选择 4 种变化中的一种进行捣乱，例如此时又选择到变化一，则系统便将 4 字节成的区块（如黑色字）内的资料进行捣乱。在第三个 4 对 1 多任务器 32 时，假设此时的控制器集成电路 42 选择到变化二的最下层“10”，系统便将 64 字节成的区块以 16 位为一单位（如深灰色字）进行捣乱。在第四个 4 对 1 多任务器 33 时，假设控制器集成电路 43 又任意选择到变化三的最下层“11”，系统便将 16 字节成的区块以 4 位为一单位（如浅灰色字）进行捣乱。因此在本实施例中，控制器集成电路 40、41、42、43 可以任意选择 4 种变化中的一种，以最下层为捣乱基础进行捣乱，每一次资料捣乱即具有任意选择的 4 种变化，本实施例包含有 4 组 4 对 1 多任务器 30—33，即具有 4^4 种变化，资料的捣乱程度更加复杂。

前述的捣乱可透过软件控制旋转（向左或向右），或作规定性的变动，且经过四层的变化捣乱，构成捣乱资料的行为模式不固定，除非资料的排列顺序经相同的变化反推还原，否则将只是外人无法了解的随机数资料。

综合上述的说明，可以归纳出下列步骤：

步骤 a、将长串位配置在划分以方块形式的相对应储存空间；

步骤 b、对 4^n 位数（n=0,1,2...）进行映像组合编码值；

步骤 c、利用一多任务器（30、31、32、33）依据编码值选择，捣乱资料的排列顺序；

步骤 d、重复步骤 b—c n 的最大次数。

如前述，本发明的资料交换器 10 将原始的资料排列顺序捣乱，此捣乱后的资料再经由随机数产生器 11 作随机加密，尽管此加密方式的行为模式固定，但地址顺序打乱，即使非法入侵者透过电压变化的观察成功破解，但行为模式不固定的排列顺序变化，将使非法入侵者无法破解。

本发明的另一优点即是以 Fractal 概念在实际的集成电路设计上，只需要设计一基本单元，即能达到均匀捣乱资料（scramble data）的目的，其架构更利于实际集成电路布局（layout）的区域（area）及时序需求（timing requirement）。

综上所述，本发明所提供的未知行为模式的资料交换运作方法及其架构，透过资料的捣乱构成未知行为模式的资料排列，能增加资料被破解的难度，对于现有的安全系统作业中存在的问题提出了有效的解决办法及对策。

OPERATION METHOD FOR A DATA EXCHANGER WITH AN UNKNOWN BEHAVE MODE AND THE ARCHITECTURE THEREOF

The present invention relates to an operation method for a data exchanger with an unknown behave mode and the architecture thereof, and more particularly, to a design of a data exchanger that will scrambling the arrangement order of the original data so that the encryption behave of the encryption security system is not fixed.

Nowadays, to establish a secure and reliable network environment and to ensure the system and the information without any illegal intruding, forging, tampering or stealing by the hackers during the network transmission, are important issues for each current network service provider and the electronic commerce. In order to achieve the object of the information security, the security system is a line of defense for the present practitioners.

The process of the security system of the conventional computer system is shown in Fig. 1. When data is written into the integrated circuit 20 through the transmission of a data exchanger 10 (or a buffer), a random number generator 11 generates a random number as the key for the data exchanger to encrypt the data. The data exchanger 10 encrypts the information by using the random number (encryption key). For the encryption processes, the encryption method for each data is absolutely the same except the random number (encryption key), namely, they have the same behave mode.

It seems that these data encryption methods are safe. The breaking of the random number (encryption key) is not easy, especially when the random number (encryption key) is 256 bits, 512 bits or 1024 bits, the breaking time for the random number (encryption key) will be increased greatly. However, another important flaw is ignored, namely, the forgoing behave mode that all the encryption processing are encrypting the data by using the random number is invariable, which causes the fatal results. In fact, the illegal intruder can deduce the behave mode of the data exchanger 10 by detecting the voltage change of the integrated circuit when every possibly present random number is inputted to the integrated circuit (as shown in Fig. 2). Actually, by using this method, there are many encryption programs that have been broken successfully, such as the ECC (Ellipse Curve Code) algorithm, RSA (Rivest, Shamir and Adleman), Block Cipher and the like. Apparently, the security of the encryption method with fixed behave mode is very worrying.

The primary object of the present invention is to provide an operation method for a data exchanger with an unknown behave mode and the architecture thereof, principally, dividing a string of data into groups, each having 4 bits; an exchanger or a buffer arranging the 4 bits in a storage area divided into 4 square shapes for scrambling; the arrangement of the position for each bit accordingly producing many changes, each of which is encoded; the encoded value of the map combination being selected by a multiplexer (4-to-1 MUX) and scrambling the data in many layers. Consequently, by

scrambling the arrangement order of the original data and diverse selectivity of the multiplexer, the encryption behave of the encryption security system is not fixed, so that the difficulty for the illegal intruder can break will be increased greatly. Therefore, the intrusion of the system can be prevented.

As mentioned above, after the data is scrambled to be reconfigured by the data exchanger of the present invention, if one multiplexer is used, every bit of the data will have four variations by the selectivity of the multiplexer, and if four multiplexers are used, every bit of the data will have 4^4 variations. The number of the multiplexers can be designed according to the need for the security level. Since the arrangement order of the data is scrambled thoroughly and evenly, and the scrambled order is one of the preceding variations, thus, even if the illegal intruder uses the forgoing way to detect the voltage change of the integrated circuit, the order of the data address can not be determined, and the deduced data will be waste data. Therefore, the flaw of the present security system can be resolved.

In order to achieve the above object, the present invention provides an operation method for a data exchanger with an unknown behave mode. The method will arrange a string of data on a storage space divided into square shapes, which constitute the respective bit, encode the map combination for each square, and scramble the data in multilayer according to the bit number of the power of 4 (0, 1, 2...), so that the position of every bit will have many variations and one of these variations can be selected to scramble the arrangement order of the original data, thus, the encryption behave of the encryption security system is not fixed.

Further, the present invention provides a architecture of a data exchanger with an unknown behave mode, characterized in that it comprises: a group of encoded multi-layer data generated by the described operation method for a data exchanger with an unknown behave mode; at least one multiplexer, for scrambling a selected appropriate layer data variation by the control of the corresponding controller integrated circuit; a random number generator, for encrypting the scrambled data randomly.

The structure and function of the present invention will be more apparent from the following detailed description thereof taken in conjunction with the accompanying drawings that illustrate specific embodiment of the invention, in which:

Fig. 1 is a schematic block diagram illustrating the process of the security system of the conventional computer system.

Fig. 2 is a schematic diagram illustrating the breaking method that detects the voltage change of the integrated circuit of the random number.

Fig. 3-1 to 3-3 are schematic diagrams illustrating the Fractal concept.

Fig. 4-1 to 4-4 are schematic diagrams illustrating the data format according to the Fractal concept of the present invention.

Fig. 5 is a schematic diagram illustrating the data format of the scrambled 256 bits data of the present invention.

Fig. 6 is an architecture diagram illustrating a data exchanger using one multiplexer according to the first embodiment of the present invention.

Fig. 7 is an architecture diagram illustrating a data exchanger using four multiplexers according to the second embodiment of the present invention.

The explanation of the denotations:

10	data exchanger	11	random number generator
20	integrated circuit	30-33	4-to-1 multiplexer
40-43	controller integrated circuit		

The essential theory of the present invention is derived from Fractal concept. As shown in Fig. 3-1, the basic architecture consists of four small triangles; any bigger block (as shown in Fig. 3-2, 3-3) comprises the following features:
1. Consisting of the basic architecture blocks.
2. The bigger blocks will ever look like the basic architecture blocks.
3. From any perspective view, all the blocks have similar shape.

The present invention applies the above features to the design of the integrated circuit that is used to control and process a data exchanger 10 or a buffer with unpredictable or predictable behave mode.

First, a 4 bits data exchanger or buffer is discussed (as shown in Fig. 4-1). After being scrambled, the bits will be arranged as a square, so that each bit (bit 0-3) will have 4 combination variations and each bit locates in one of the corner of the square (0, 1, 2, 3 shown in the figure denote bit 0-3).

In the present embodiment, one 4-to-1 multiplexer 30 (4-to-1 mux) is used (as shown in Fig. 6) to control each combination. For the detailed description, we can provisionally use:

"00" denotes

0	1
3	2

"01" denotes

1	0
2	3

"10" denotes

3	2
1	0

"11" denotes

2	3
1	0

That is to say, when the 4-to-1 multiplexer 30 selects "00", the 4 bits data exchanger will be scrambled by the multiplexer as:

0	1
3	2

Also, after being scrambled, the map combinations of "00", "01", "10" and "11" will be redefined and known by only the developer.

The 4 bits architecture can be expanded upwards, as shown in Fig. 4-2, based on the 4 bits square architecture, four of the 4 bits square architecture can form a 16 bits block, and each square that denotes 4 bits formerly can be regarded as 1 bit, thus, the square can be scrambled and denoted as:

0	1
3	2

(as shown in Fig. 4-2 in dark gray words), so that a scrambled 16 bits data is formed.

Then, based on the 16 bits block, four of the 16 bits square architecture can form a 64 bits block, and each square that denotes 16 bits formerly can be regarded as 1 bit, thus, the square can be scrambled and denoted as:

0	1
3	2

(as shown in Fig. 4-3 in light gray words), so that a scrambled 64 bits data is formed.

In this way, based on the 64 bits block, four of the 64 bits square architecture can form a 256 bits block, and each square that denotes 64 bits formerly can be regarded as 1 bit, thus, the square can be scrambled and denoted as:

0	1
3	2

(as shown in Fig. 4-4 in contour words), so that a scrambled 256 bits data is formed.

Thus, Fig. 4-1 to 4-4 are all formed by the 4 bits square architecture in the Fig. 4-1 (Namely, it have the same feature as the Fractal concept.). As a result, we can define a data buffer with layers, 16 bits is 4^2, 64 bits is 4^3, and 256 bits is 4^4, namely, the number 2, 3, and 4 denote the layer of the data buffer. For example, for a 4 bits data buffer, there is only one layer combination for each bit; a 64 bits data buffer (4^3) thus comprises the architecture with 3 layers.

As mentioned above, each layer can be divided into 4 equal parts, therefore, for each equal part, the combination number "00", "01", "10" and "11" can be used to specify the data for each layer. Consequently, a 4-to-1 multiplexer 30 can be used for control of the specifying layer and block, and the original data is scrambled or reorganized with the 4 possible variation combinations. These variation combinations can be selected by the developer in advance to predefine the correlation of each layers, furthermore, the combination of each layer can be defined according to the following principle:
"If a combination is selected for a layer, the most furthest combination from the current combination will be selected for the next layer."
According to this principle, even a 256 bits buffer will be limited to 4 variations, and can be controlled by the 4-to-1 multiplexer 30.

The following table is a correlation table, which provides the logic control for a 256-bits data buffer; therefore, each bit can be denoted as a 4-layer combination:

Variation	Uppermost layer	Middle upper layer	Middle lower layer	Lowest layer
1	00	10	11	01
2	01	11	00	10
3	10	00	01	11
4	11	01	10	00

Taking a 256 bits data as an example, it can be supposed that the code for the formed square based on 4 bits according to the above method is:

1	0
2	3

(as shown in black words); we can suppose that the code for the 16 bits square formed by 4 of the 4 bits squares is:

2	3
1	0

(as shown in dark gray words); we can suppose that the code for the 64 bits square formed by 4 of the 16 bits squares is:

3	2
1	0

(as shown in light gray words); we can further suppose that the code for the 256 bits square formed by 4 of the 64 bits squares is:

0	1
3	2

(as shown in contour words). The reorganized data is shown in Fig. 5. Therefore, the arrangement order of such data is scrambled, and the scrambled data obtained by the illegal intruder will be waste data because the scrambling rule cannot be known except for the program developer.

The architecture diagram of a data exchanger of the present invention is shown in Fig. 6. Herein, the 256 bits (16 bits ×16 bits) data will be taken as an example for N bits × N bits data. According to the forgoing theory, the 256 bits data can be divided as a 4-layer structure (4 layers for 4 bits, 16 bits, 64 bits and 256 bits), and one 4-to-1 multiplexer 30 can be used to select variations. Moreover, the enable of the 4-to-1 multiplexer 30 is controlled by the controller integrated circuit (controller IC) 40 (that can be controlled by software). According to variation 1, the controller integrated circuit 40 randomly selects one of the variations and scrambles the data, for example, if the "01" is selected for the lowest layer, the system will scramble the data in the block that is formed by 4 bits (as shown in black words), so that the arrangement order of each bit of the original data will be scrambled, or according to variation 1, the controller integrated circuit 40 randomly selects the "11" for the middle lower layer, the system will scramble the data by using the 16 bits formed block as a unit (as shown in dark gray words). The rest may be deduced by analogy, therefore, in the present embodiment, there are four variable scrambling modes for the forgoing bits data.

As shown in Fig. 7, in the present embodiment, 4 groups of the 4-to-1 multiplexer 30-33 are used, and the 4 bits (namely, the lowest layer of the each variation in the above table will be the basic unit for the scrambling. Moreover, for each 4-to-1 multiplexer 30, 31, 32 and 33, the controller 40, 41, 42 and 43 can randomly select variation, for example, for the first 4-to-1 multiplexer 30, the controller integrated circuit 40 selects the variation 1 and the "01" is selected for the lowest layer, the system will scramble the data in the block that is formed by 4 bits (as shown in black words), so that the arrangement order of each bit of the original data will be scrambled. When the scrambled data is through the second 4-to-1 multiplexer 31, the controller integrated circuit 41 can randomly select one of the 4 variations and scramble the data, for example, if the variation 1 is selected again this time, the system will scramble the data in the block that is formed by 4 bits (as shown in black words). When through the third 4-to-1 multiplexer 32, supposed that the "10" is selected for the lowest layer of the variation 2 by the controller integrated circuit 42, the system will scramble the data by using 16 bits as unit in the block that is formed by 64 bits (as shown in dark gray words). When through the fourth 4-to-1 multiplexer 33, supposed that the "11" is further selected for the lowest layer of the variation 3 by the controller integrated circuit 43, the system will scramble the data by using 4 bits as unit in the block that is formed by 16 bits (as shown in light gray words). Therefore, in the present embodiment, the controller integrated circuit 40, 41, 42 and 43 can randomly select one of the 4 variations and scramble the data based on the lowest layer, and each data scrambling has 4 randomly selected variations, consequently, for the 4 groups of the 4-to-1 multiplexer 30, 31, 32 and 33 in the present embodiment, there is 4^4 variations and the degree of the data scrambling becomes more complex.

For the forgoing scrambling, the rotation (leftwards or rightwards) or specified variation can be controlled by the software. Moreover, after the four layer variation and scrambling, the behave mode of the data scrambling is not fixed, consequently, the data will be some random numbers that can not be understood by the stranger unless the arrangement order of the data is restored through the reverse deduction that uses the same variation as the scrambling.

To summarize the above explanation, the following steps can be included:
Step a: arrange a string of data on a storage space divided into square shapes, which constitute the respective bit,
Step b: encode the map combination for the bit numbers of the 4^n ($n = 0, 1, 2\ldots$).
Step c: according to the selection of the code, a multiplexer (30, 31, 32 and 33) is used to scramble the arrangement order of the data.
Step d: repeat the step b – c until the maximum n is reached.

As mentioned above, the data exchanger 10 of the present invention scrambles the arrangement order of the original data, and then, the random number generator 10 encrypts the scrambled data randomly. Although the behave mode of the encryption method is fixed, the order of the address is scrambled. Consequently, even if the illegal intruder can break successfully by detecting the voltage change, the illegal intruder can not break the unfixed behave mode for the variation of the arrangement order.

The present invention has another advantage of that the Fractal concept is used for the design of the integrated circuit. Consequently, the object to scramble data evenly can be reached as long as a basic unit is designed. Moreover, the architecture is more suitable for the area and timing requirement for the layout of the practical integrated circuit.

In summary, the operation method for a data exchanger with an unknown behave mode and the architecture thereof, which are provided by the present invention, can increase the difficulty to break the data by the data scrambling that generates the data arrangement with an unknown behave mode. This is an efficient solution and strategy for the existing problem in the operation of the conventional security system.

WHAT IS CLAIMED:

1. An operation method for a data exchanger with an unknown behave mode, characterized in that: arrange a string of data on a storage space divided into square shapes, which constitute the respective bit, encode the map combination for each square, and scramble the data in multi-layer according to the bit number of the power of 4 (0, 1, 2...), so that the position of every bit will have many variations and one of these variations can be selected to scramble the arrangement order of the original data, thus, the encryption behave of the encryption security system is not fixed.

2. The operation method for a data exchanger with an unknown behave mode according to claim 1, characterized in that the scrambling step comprises controlling the leftwards or rightwards rotation or specified variation by the software.

3. The method for a data exchanger with an unknown behave mode according to claim 1, characterized in that:
the selectivity of the variation is that the combination is selected for a layer, the furthest combination from the current combination will be selected for next layer.

4. The method for a data exchanger with an unknown behave mode according to claim 1, characterized in that the layer and variation of the scrambling depend on the bit number of the data.

5. The method for a data exchanger with an unknown behave mode according to claim 1, characterized in that the method comprises the following steps:
Step a: arrange a string of data on a storage space divided into square shapes, which constitute the respective bit,
Step b: encode the map combination for the bit numbers of the 4^n ($n = 0, 1, 2...$).
Step c: according to the selection of the code, a multiplexer (30, 31, 32 and 33) is used to scramble the arrangement order of the data.
Step d: repeat the step b – c until the maximum n is reached.

6. A architecture for a data exchanger with an unknown behave mode, characterized in that it comprises:
a group of encoded multilayer data generated by the operation method for the data exchanger with an unknown behave mode according to claim 1;
at least one multiplexer, for scrambling a selected appropriate layer data variation by the control of the corresponding controller integrated circuit;
a random number generator, for encrypting the scrambled data randomly.

7. The architecture for a data exchanger with an unknown behave mode according to claim 6, characterized in that the multiplexer is a 4-to-1 multiplexer.

ABSTRACT

The present invention relates to an operation method for a data exchanger with an unknown behave mode and the architecture thereof, principally, dividing a string of data into groups, each having 4 bits; an exchanger or a buffer arranging the 4 bits in a storage area divided into 4 square shapes for scrambling; the arrangement of the position for each bit accordingly producing many changes, each of which is encoded; the encoded value of the map combination being selected by a multiplexer (4-to-1 MUX) and scrambling the data in many layers. Consequently, by scrambling the arrangement order of the original data and diverse selectivity of the multiplexer, the encryption behave of the encryption security system is not fixed, so that the difficulty for the illegal intruder can break will be increased greatly. Therefore, the intrusion of the system can be prevented.

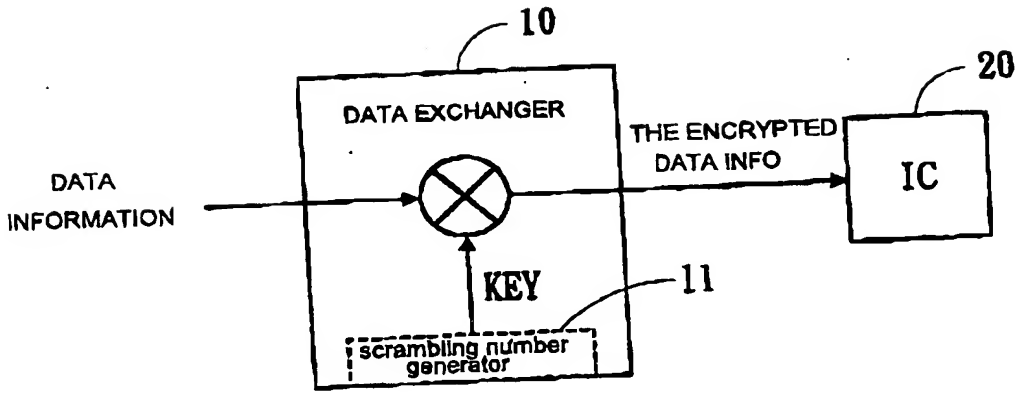


FIGURE 1

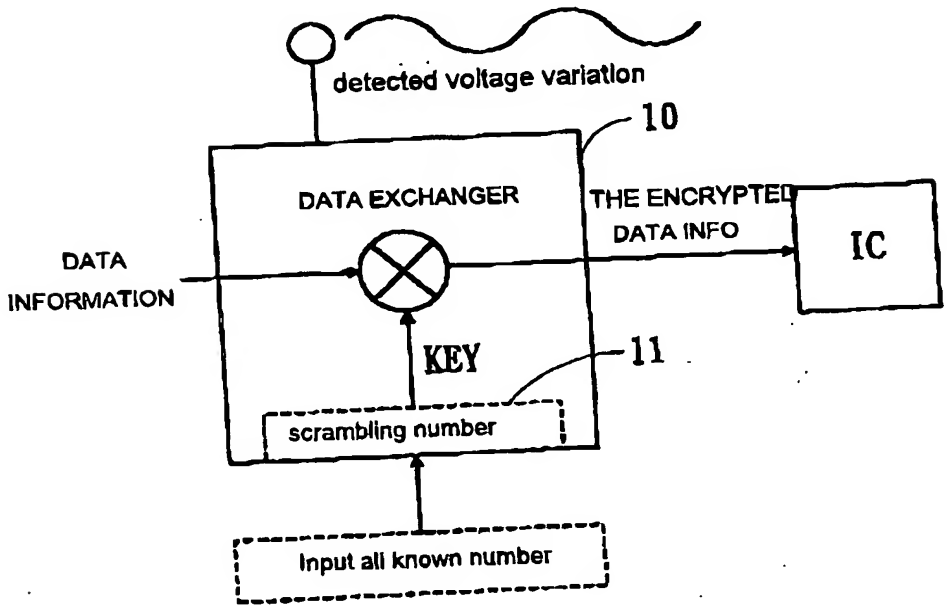


FIGURE 2

FIGURE 3-1

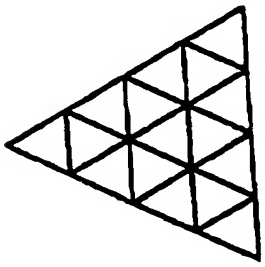


FIGURE 3-2

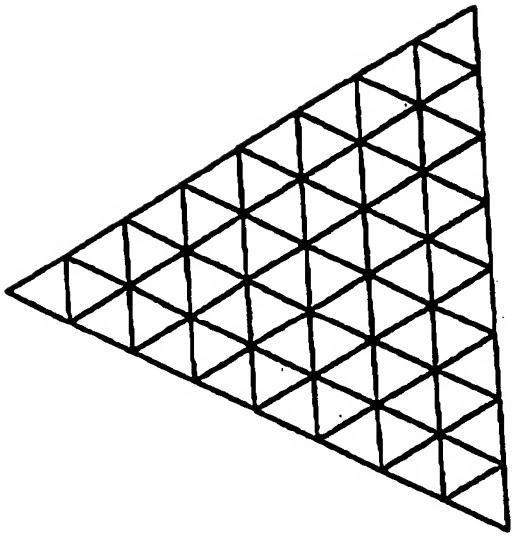
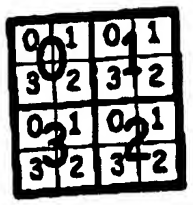


FIGURE 3-3

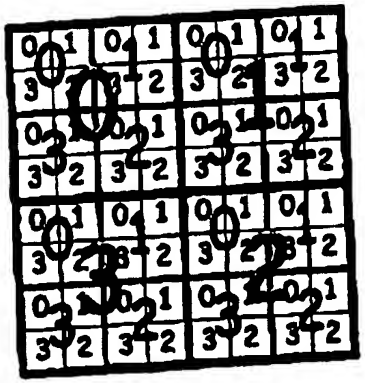
4-bit

FIGURE 4-1



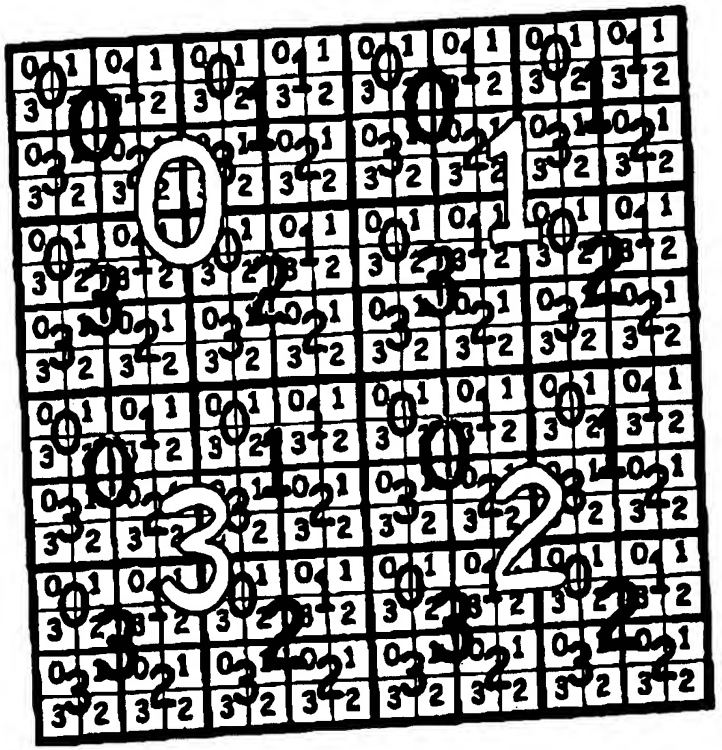
16-bit

FIGURE 4-2



64-bit

FIGURE 4-3



256-bit

FIGURE 4-4

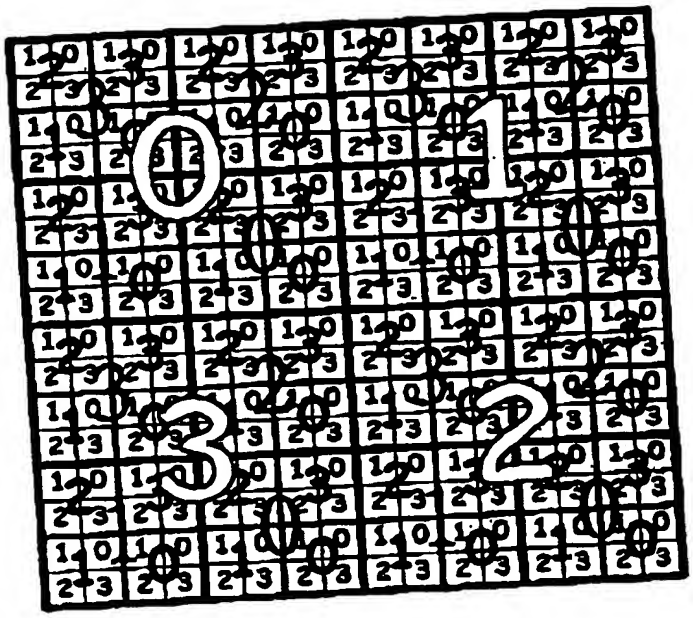


FIGURE 5

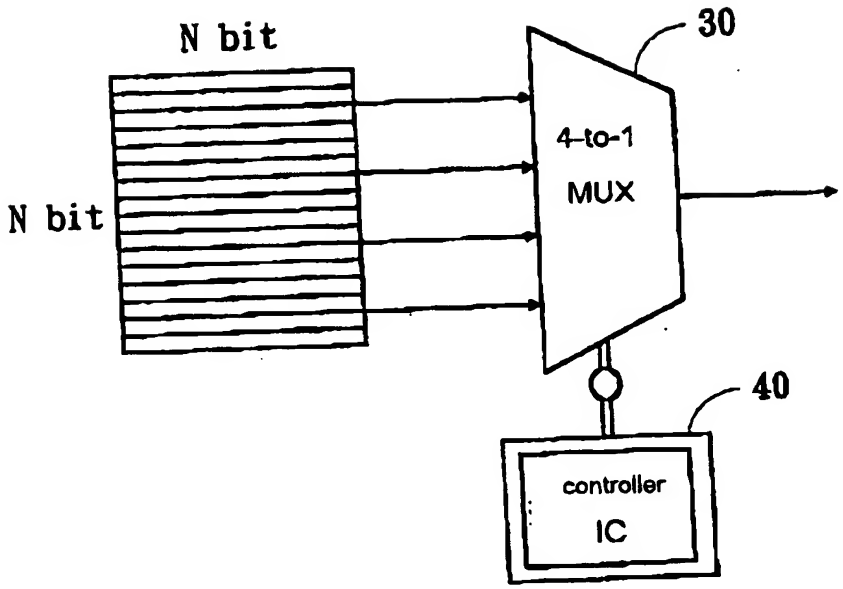


FIGURE 6

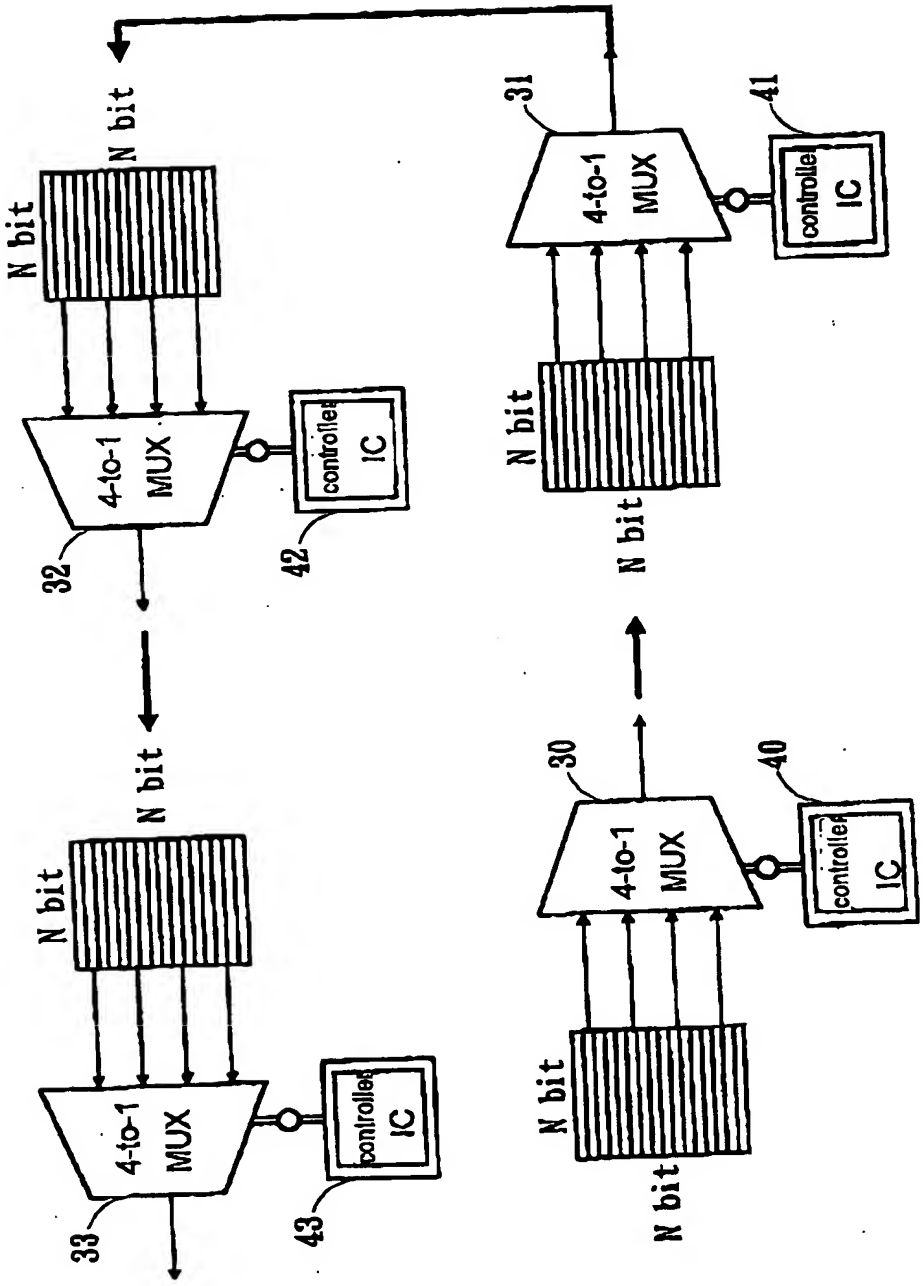


FIGURE 7